FORTINET
High Performance Network Security

FortiHypervisor - Administration Guide

Version 1.1

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Thursday, October 19, 2017

FortiHypervisor - Administration Guide

Version 1.1.0

Change Log

Date	Change Description
2017-10-18	Minor formating changes and typo corrections
2016-08-00	Initial release for 1.0.0

TABLE OF CONTENTS

Introduction

The FortiHypervisor Hybrid Virtual Appliance enables rapid service delivery for enterprise and MSPs through the use of virtualization technology. Built to deliver multiple virtualized network functions (VNFs), FortiHypervisor consolidates advanced networking and security services, eliminating the need for multiple CPE while enabling on-demand service delivery.

FortiHypervisor is available as Fortinet SPU accelerated hybrid appliances and also in software format for install on generic x86 platforms. In appliance format, a powerful Intel processor combined with SPU hardware acceleration delivers the high security performance that customers have come to expect from Fortinet. Ample storage and memory produce excellent compute, network and security performance for the most intensive tasks.

FortiHypervisor supports an industry leading range of virtual network functions with native Fortinet VNFs and support for standards based thirty party VMs.

Foundations

The FortiHypervisor firmware is built of the following core components:

1. **FortiOS** - The FortiOS in this case has been striped of a number of the major feature that are at home on a firewall but have no place in a platform for hosting virtual devices. The CLI structure looks similar to the regular FortiOS, but if you dig further into the code you will notice differences.
2. **QEMU** - QEMU 2.41 has been integrated into the firmware
3. **KVM Kernel Module for QEMU** - This component has been integrated into QEMU since v.1.3
4. **FortiOS 5.4 GUI** - The GUI has the same look and feel of the GUI from FortiOS 5.4, but due to the different purpose and therefore functions required, the menu items of the GUI are almost completely different.

Form factors

FortiHypervisor is available in two form-factors to allowing customers to select the most appropriate solution for their requirements.

Both approaches to FortiHypervisor use KVM-based hypervisor

Appliance

FortiHypervisor comes in a range of physical appliances suitable for small office / retail deployments (vCPE) all the way up to the datacenter and MSP network core. The models come with different performance ratings, amounts of Hard Drive space, RAM and network access ports.

- Runs on Fortinet x86 hardware with optional FortiASIC capabilities depending on model
- FortiGate VM available as Virtual Network Function (VNF), with FortiASIC accelleration

- Can run other Fortinet and 3rd party VMs
- Supports service orchestration via 3rd party SDN/NFV
- Several hardware models

Virtual Appliance (ISO)

FortiHypervisor is available as a bare metal hypervisor ISO image which can be installed on selected whitebox hardware.

- Runs on a generic 3rd party x86 appliance (whitebox)
- Can run other Fortinet and 3rd party VMs
- On hardware with sufficient resources can run FortiMail-VM and FortiSandbox-VM
- Supports service orchestration via 3rd party SDN/NFV
- No ASIC offloading
- Customer is responsible for hardware

Any selected hardware should be validated against the supported hardware list and should meet the minimum hardware specification lists below.

Whilst a minimum specification is provided, consideration should be made towards the VMs which will be installed as these may have additional performance and resource requirements.

If unsure, please validate your hardware selection with Fortinet Support before proceeding.

Supported hardware

There isn't a complete list of certified vender specific hardware but there is component support for the following compatible devices:

CPU	Network	SCSI
Intel	E1000/E1000e	MEGARAID_SAS
AMD	EGB	MPT2SAS
	IXGBE	FUSION_SAS
	TG3	HPSA
	BNX2	
	RTL8169	

Any hardware not listed as supported should be submitted to Fortinet as an NFR for consideration for inclusion.

NPU support

The following requirements must be met in order for traffic to be accelerated on the FortiHypervisor appliance:

- Appliance must contain an NP6 ASIC (e.g. FHV-500D or FHV-2500E)
- VM vNIC model must be set to VirtIO
- VM interface must be set to a pass through virtual switch

You can verify if traffic is being offloaded by running `diagnose sys session list` in the guest FortiOS VM.

Offloaded output will look like this:

```
serial=00000026 tos=ff/ff app_list=0 app=0 url_cat=0
dd_type=0 dd_mode=0
npu_state=0x000c00
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=130/131, ipid=131/130,
    vlan=0x0000/0x0000
vlifid=131/130, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=0/0
total session 1
```

NP Limitations

Whilst the majority of NP functions have been exposed for use by the guest FortiOS, some functions are not yet implemented. Currently all features of the NPU are supported by FortiOS KVM with the exception of:

- CAPWAP offloading
- NTrubo offloading
- IPTunnel offloading

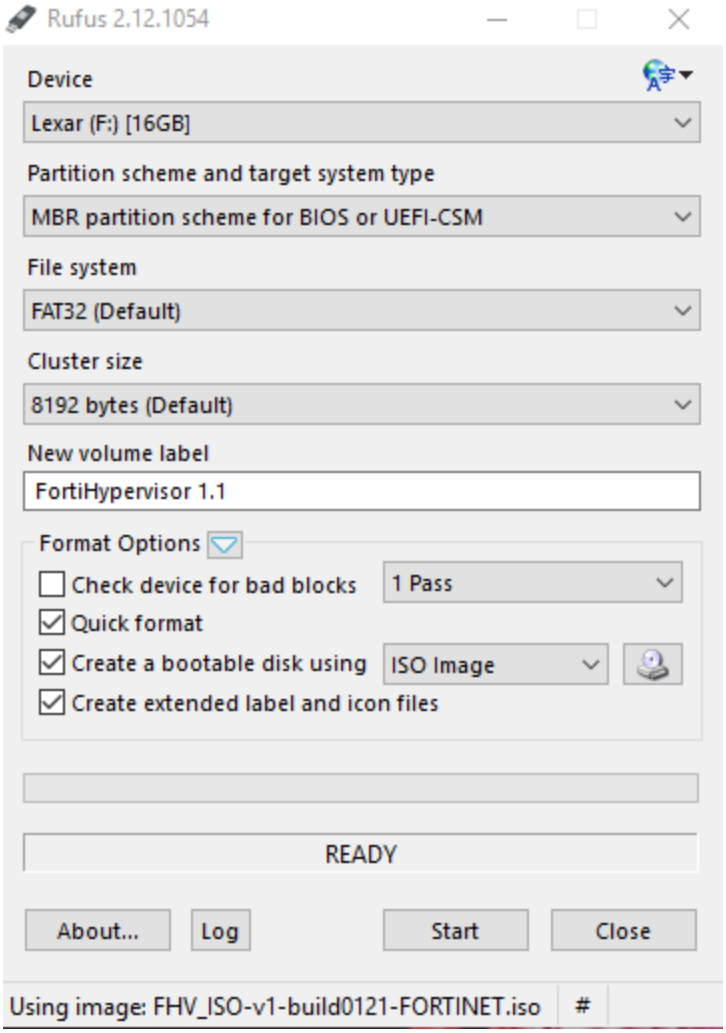
Installing the ISO

FortiHypervisor is available in ISO format for installation on generic “whitebox” hardware. Download this for the Fortinet support site and burn to a CDROM/DVD for installation. If a CDROM is not available to perform the installation, follow the information in the section.

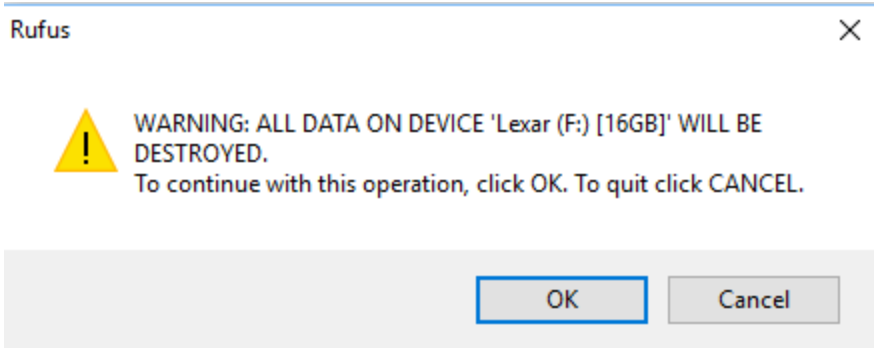
Creating USB boot media

It is possible to write FortiHypervisor to a USB device for installation purposes. To achieve this, download a copy of the USB creation utility Rufus https://rufus.akeo.ie/.

1. Select the USB device to which to install the ISO Bootable Disk.
2. Select **Create a bootable disk using ISO image** and click the CD icon to select the source as the downloaded FortiHypervisor ISO image.



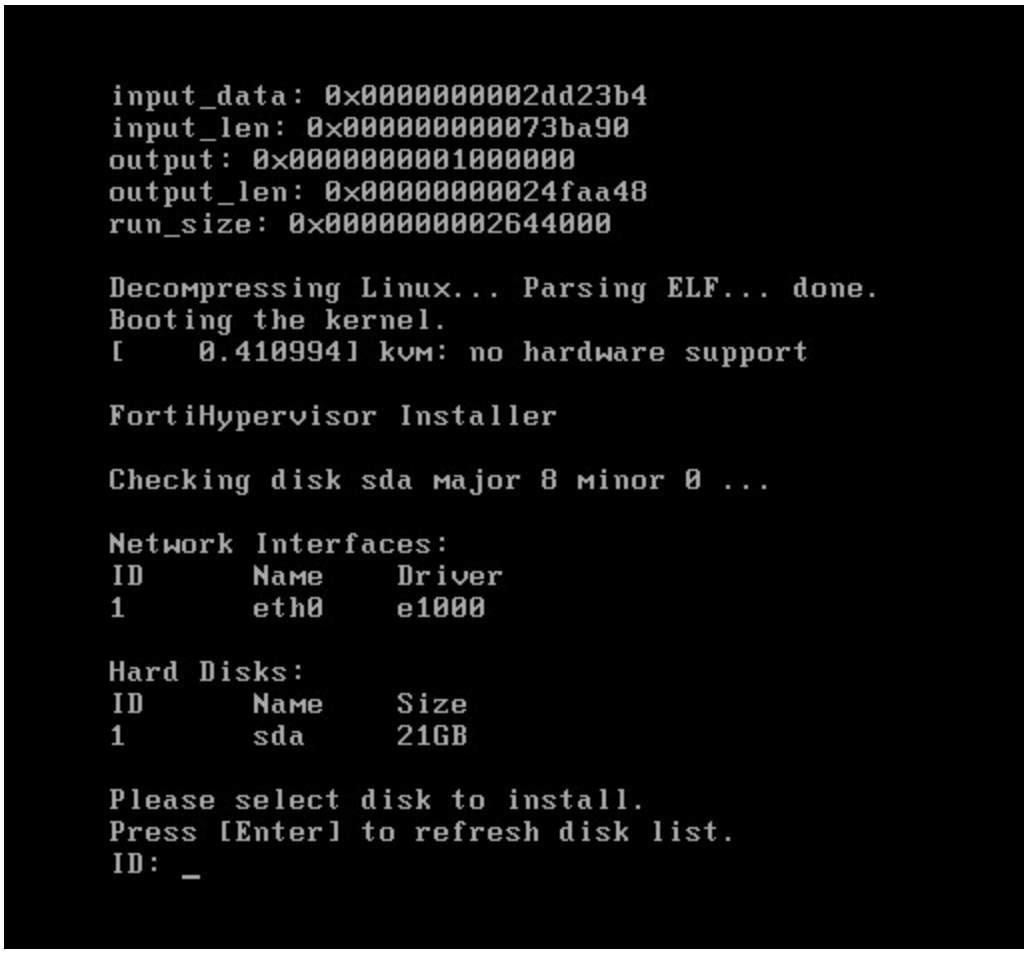
3. Select start and validate the settings before clicking OK to continue with the install of FortiHypervisor to the USB media.



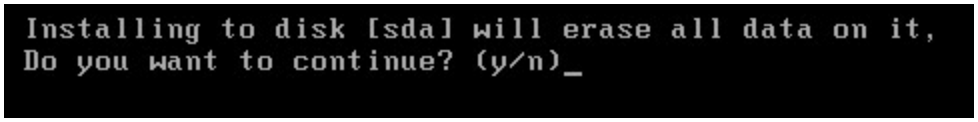
Once complete, this USB device can be used to install FortiHypervisor.

Installing FortiHypervisor

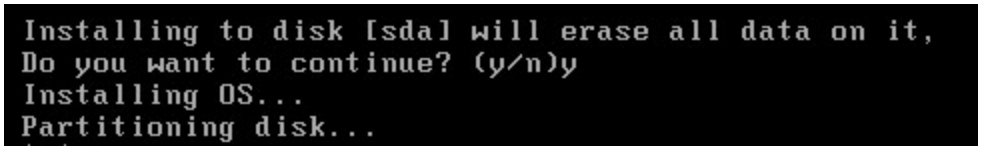
1. Boot your device with either the CDROM (ISO) or USB installation media. Note that you may need to consult your hardware manufacturer's guide to change the default boot order.
2. Once booted, assuming the network and disks have been correctly identified, the following prompt will be displayed.



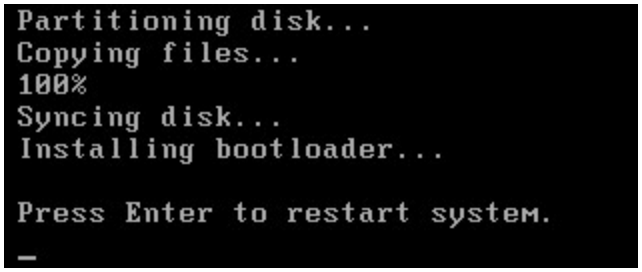
3. Select the correct disk on which to install FortiHypervisor



4. Accept the prompt to continue (assuming this is the correct disk and you are happy to lose any data currently stored.



5. The disk partition process will begin. After several minutes, the installation process should complete.



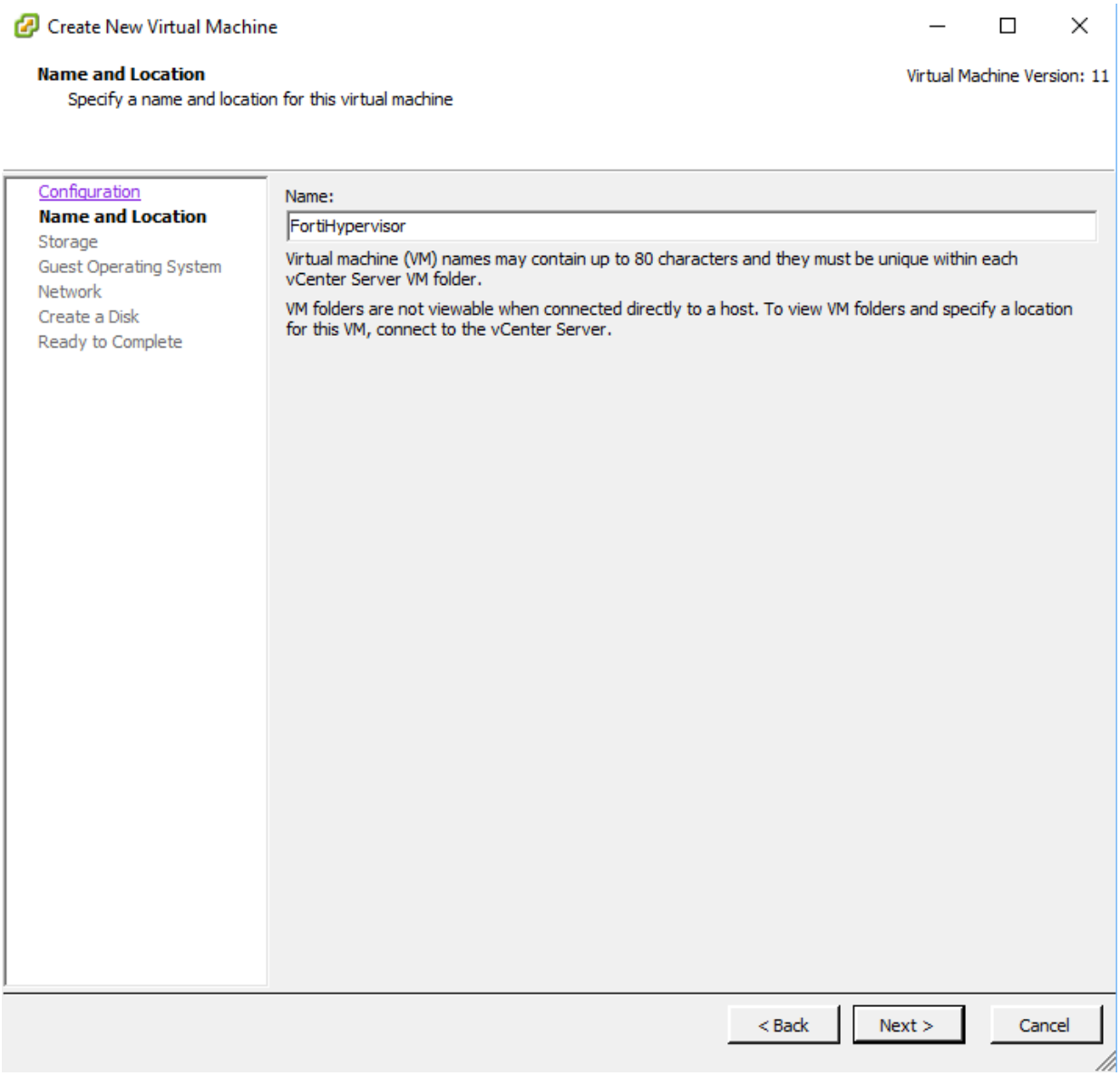
6. Follow the instructions on screen to complete the install process and reboot.
7. Continue the configuration process as per hardware appliances.

Installing FortiHypervisor in VMWare ESXi

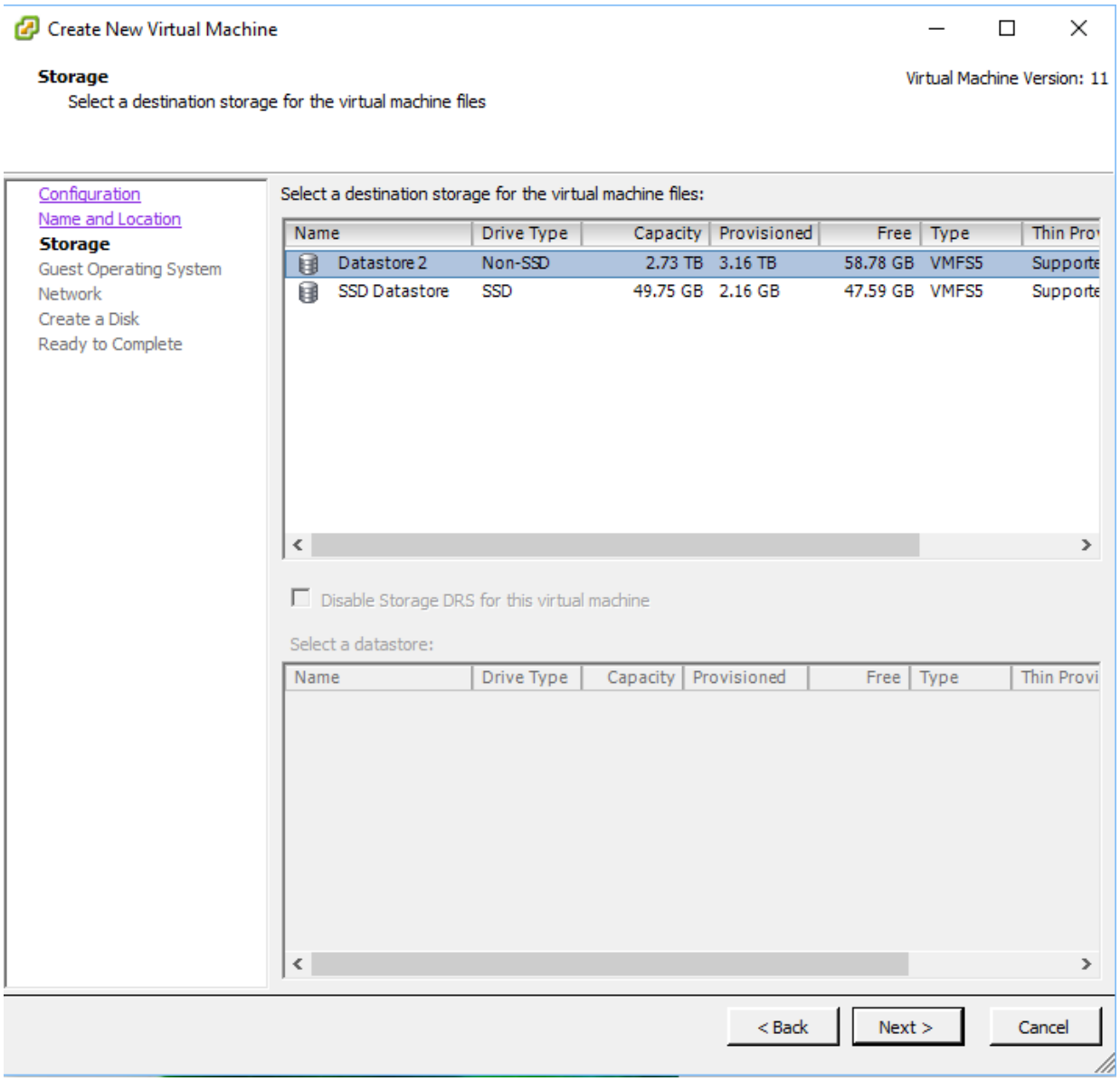
Whilst not recommended for general use, it is possible to install FortiHypervisor into an existing hypervisor such as VMWare ESXi. This is useful for demo purposes and testing.

To install FortiHypervisor in VMWare ESXi, follow these steps:

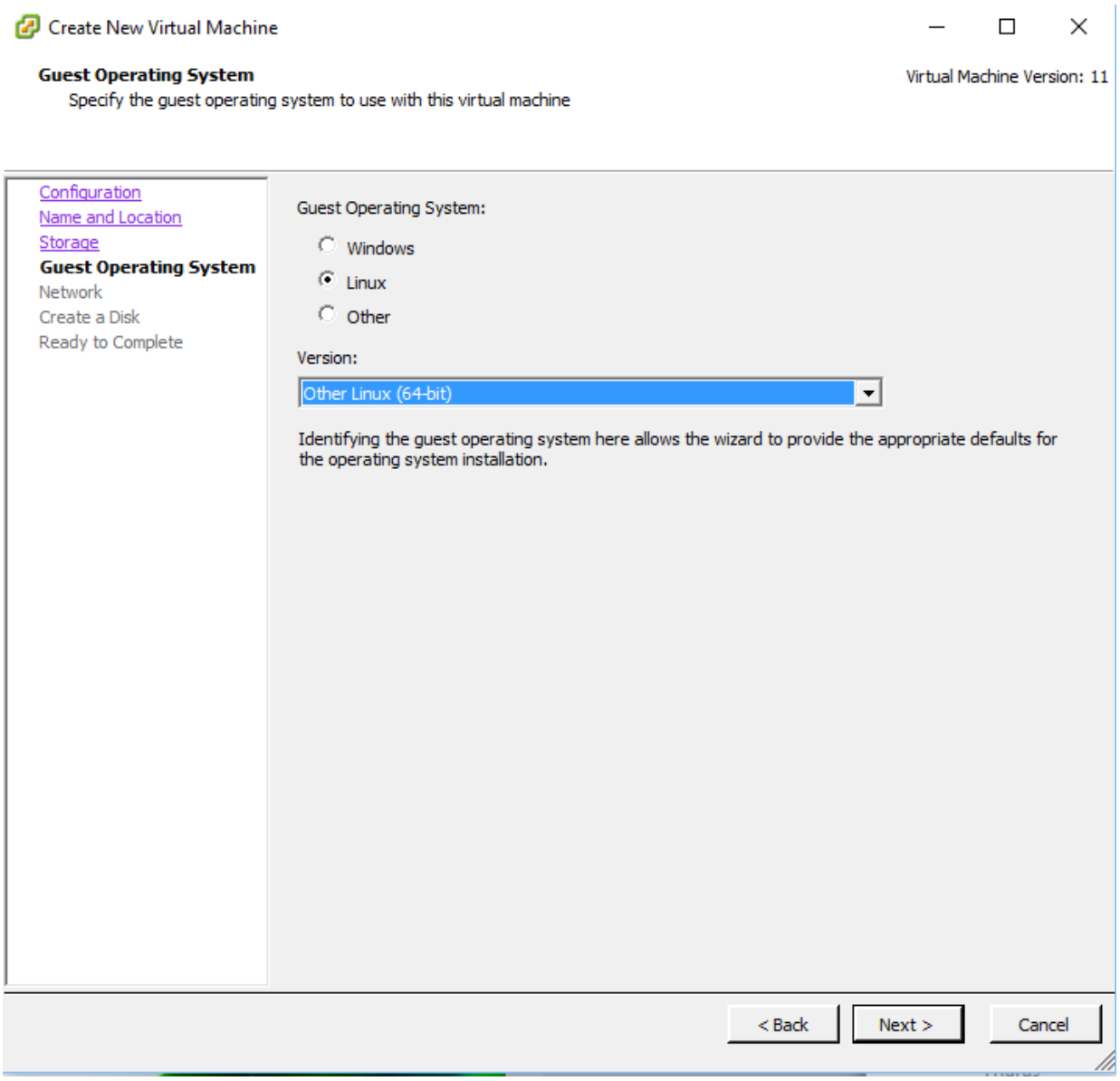
1. Create a new VM



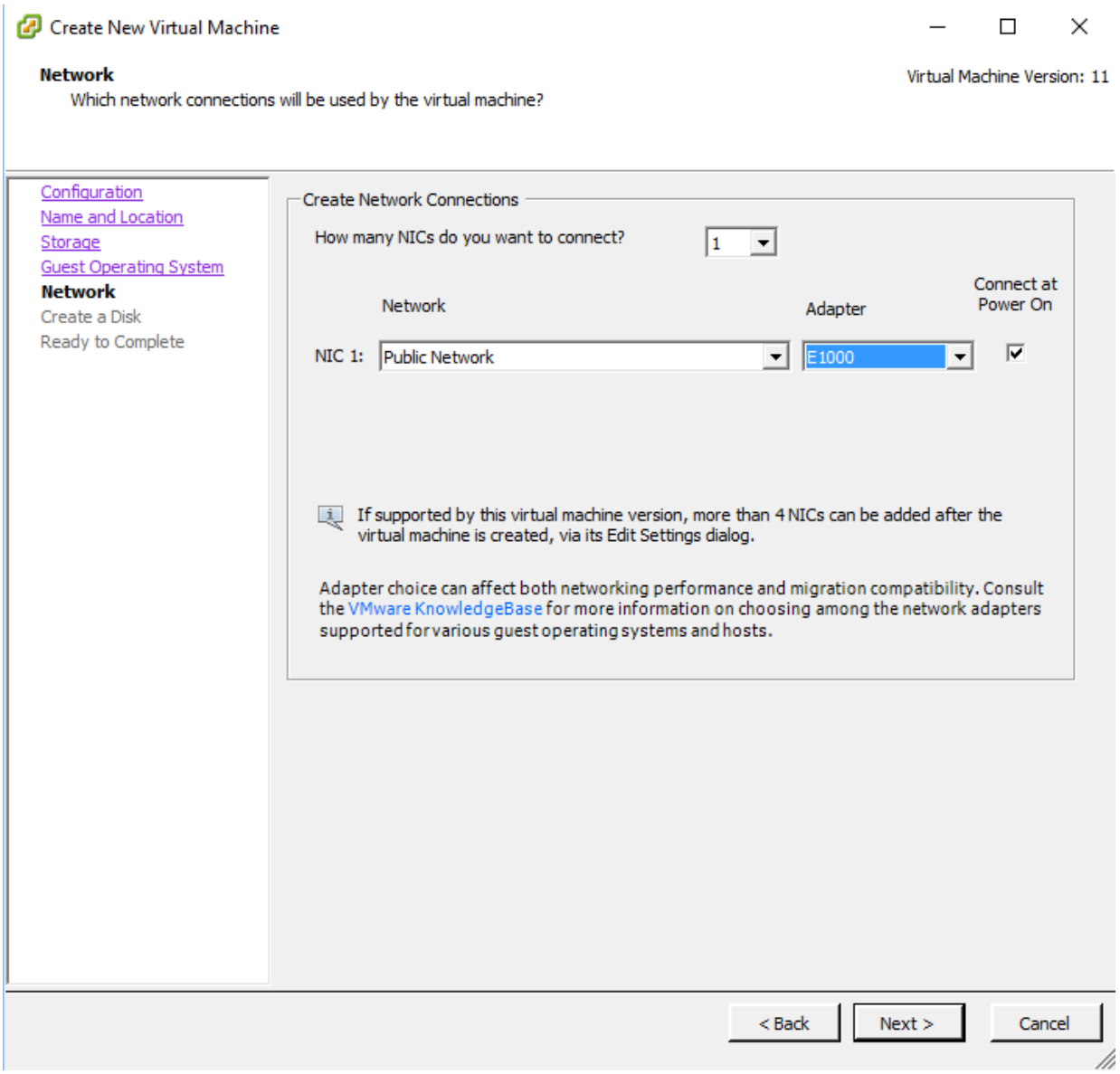
2. Select the storage destination.



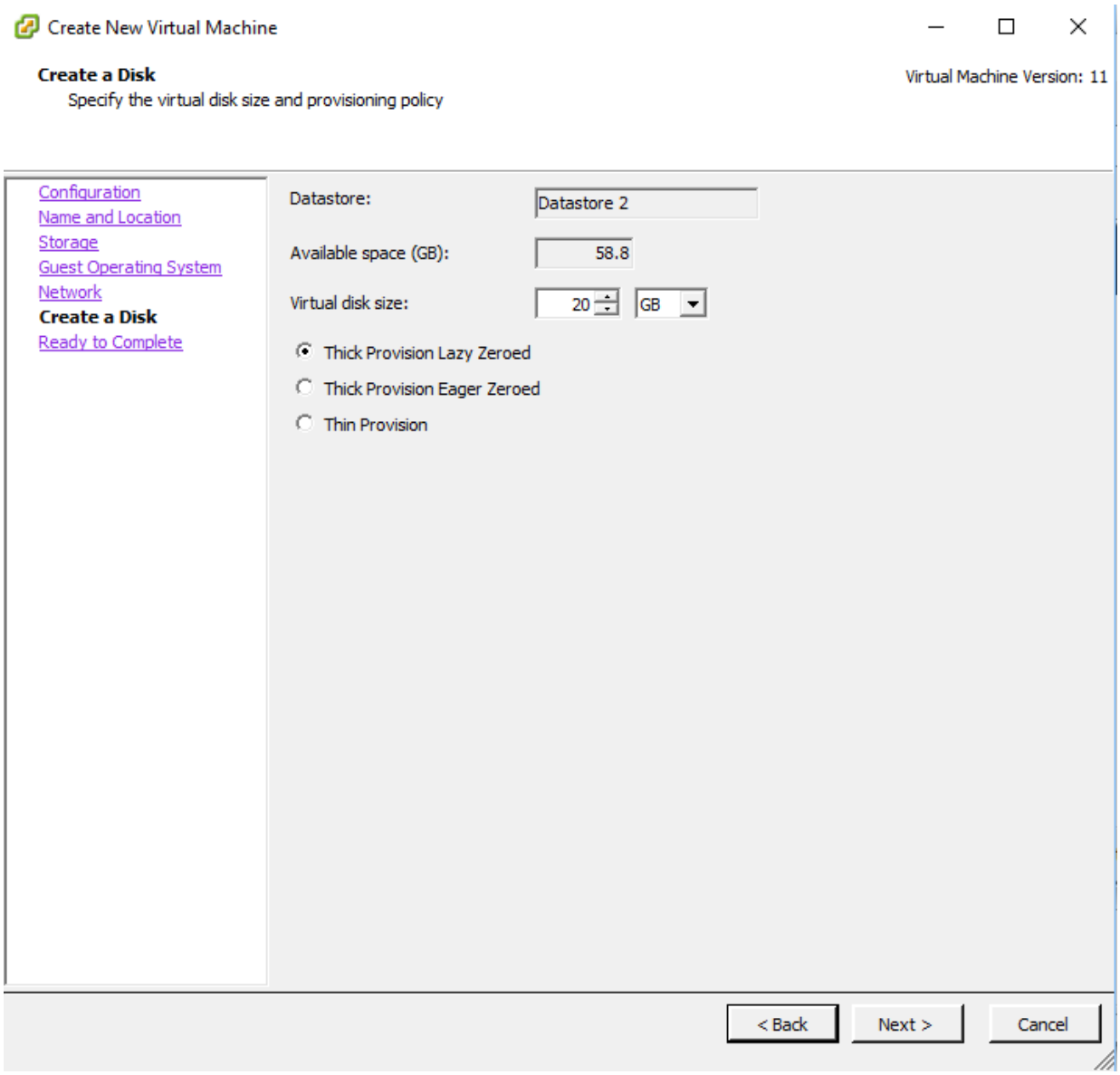
3. Set the Guest Operating System to Other Linux (64 bit)



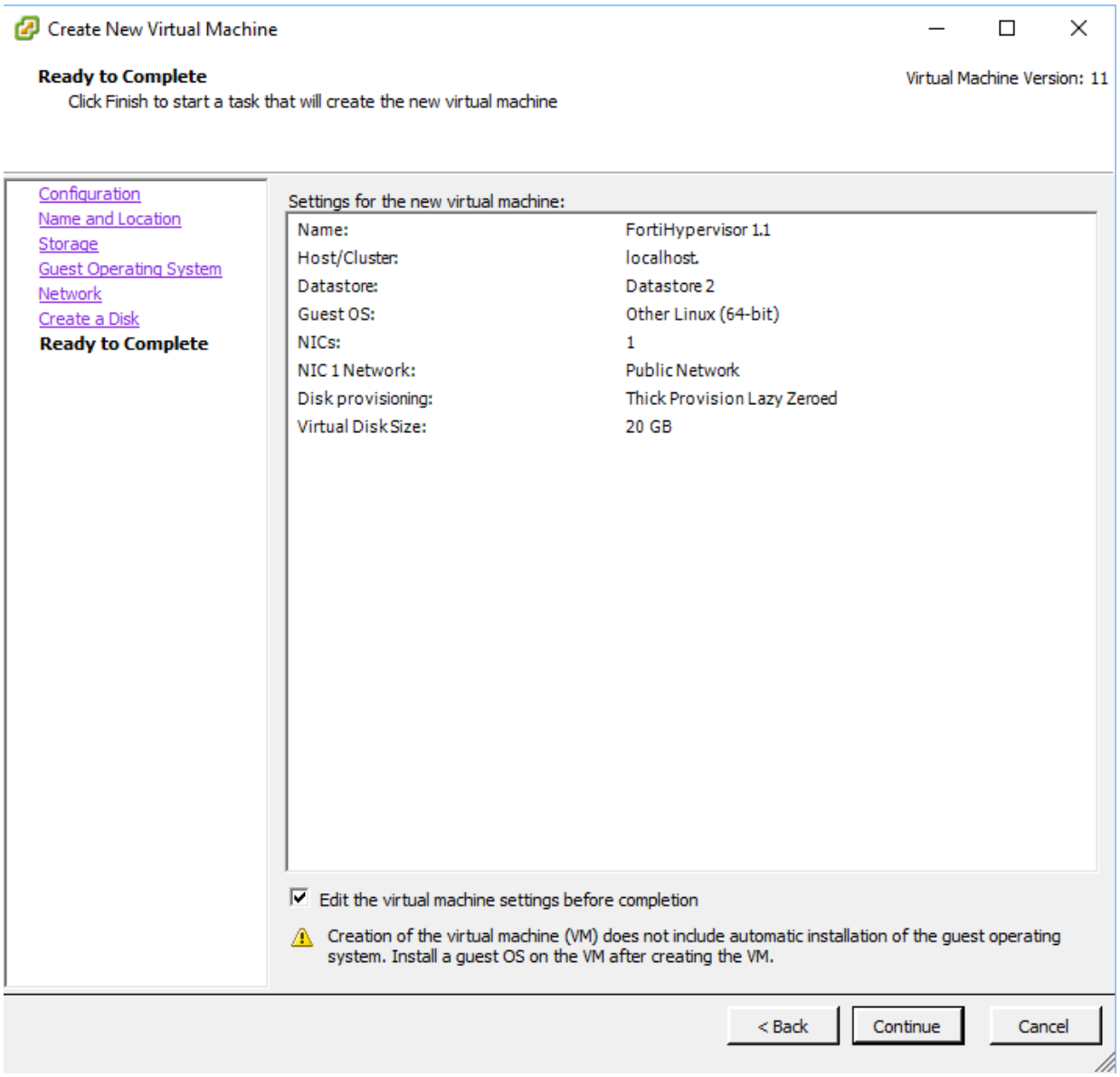
4. Assign network resources to the VM instance.



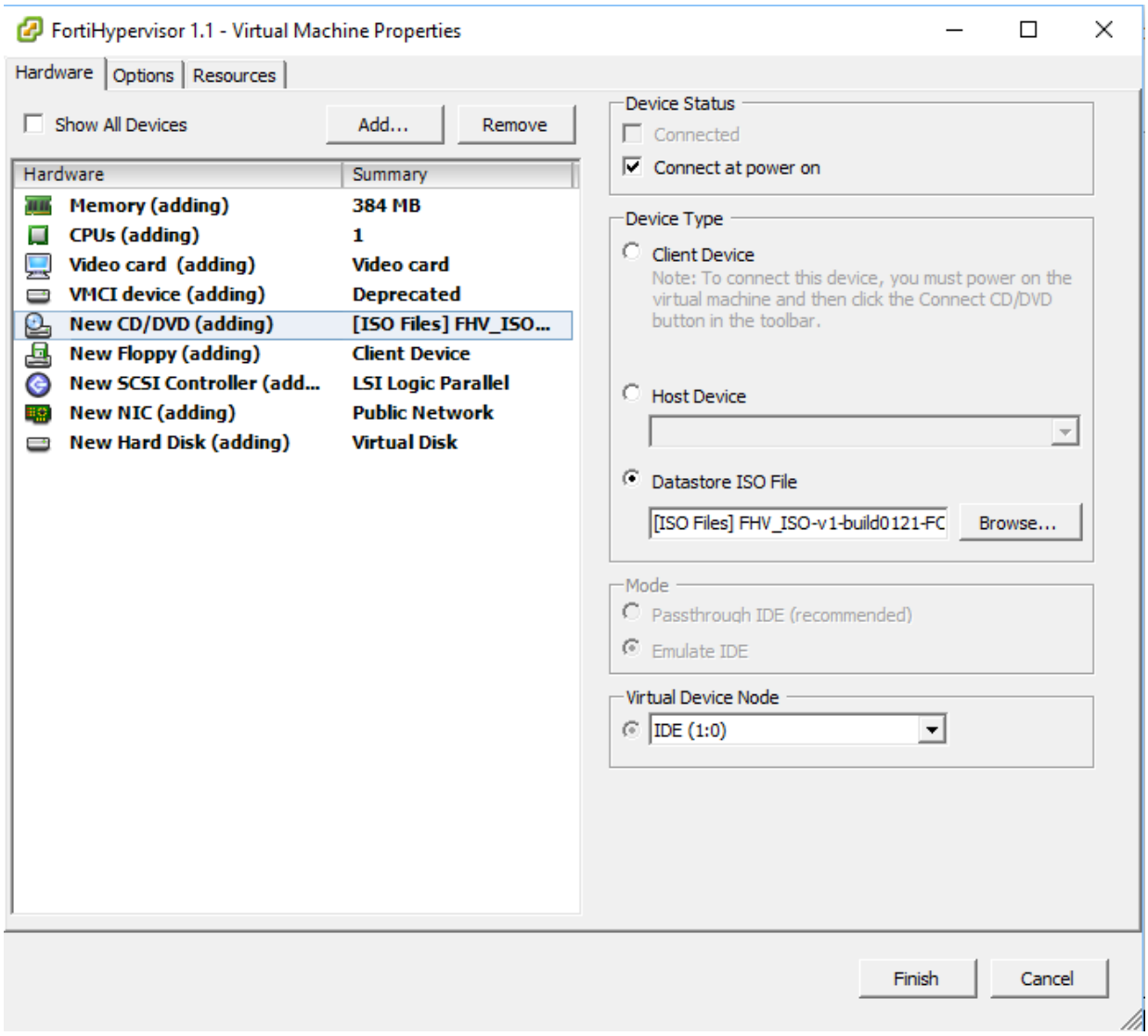
5. Assign disk resource to the VM instance



6. Review the configuration, “edit the virtual machine settings before completion” and click continue.



7. Configure the Datastore ISO file to point to the FortiHypervisor install ISO and select Connect at power on.



8. Follow the install process detailed in the section “Installing FortiHypervisor”.

Configuration

This section discusses the installation and use of FortiHypervisor in your network, after completion of the initial setup outlined in the FortiHypervisor model's Quick Start Guide. The section also provides troubleshooting tips and links to other resources.

The following example content is based on the FortiHypervisor 500D. The process is similar for other FortiHypervisor appliances; however variations in model specification may alter which interface settings are available.

The default IP address of the FortiHypervisor **mgmt1** interface is set to 192.168.1.99/24. To perform the initial configuration, connect a device to **mgmt1** Configure the device with an IP address to 192.168.1.1/24. The FortiHypervisor should be accessible via SSH or the Web GUI.

The default value for **Username** is `admin` and the **Password** is null or blank, depending on your preferred terminology.

Use the GUI or CLI to set the permanent IP address configuration.

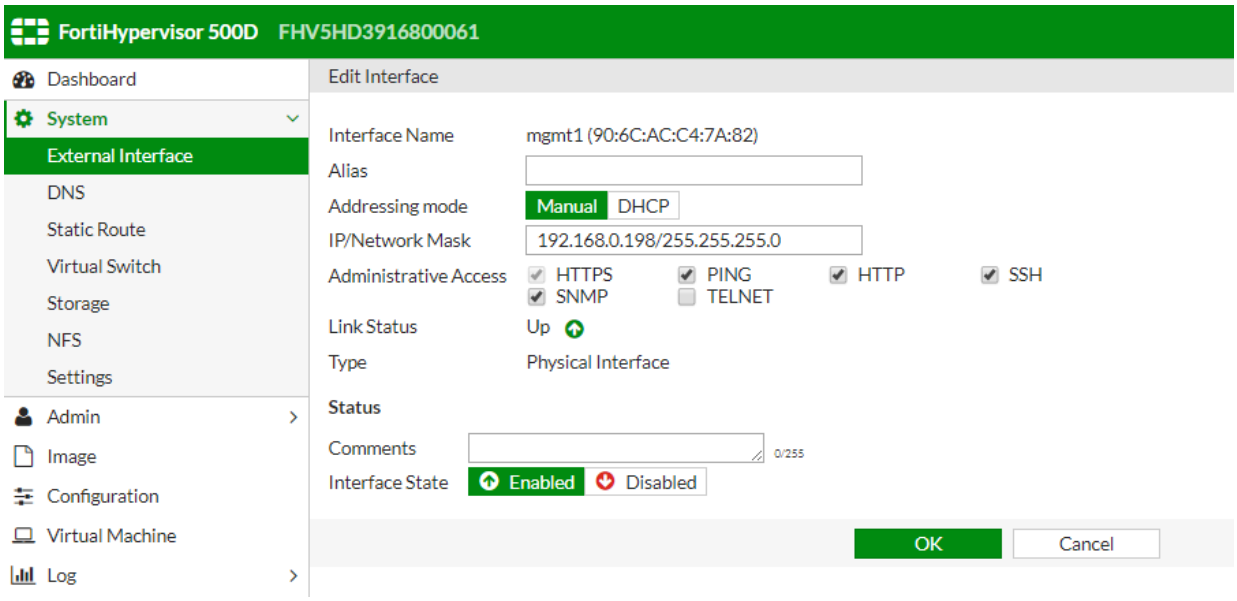
The initial configuration may be performed on the serial console. Please the quick start guide for details. http://docs.fortinet.com/fortihypervisor/hardware/

Configuring the Management IP

The numbered ports on the FortiHypervisor are normally associated with Virtual Switches or subnets for the VMs. While it is possible to connect to the FortiHypervisor through these interfaces, the primary access points are usually the **mgmt1** or **mgmt2** ports. Unless your LAN happens to coincide with the default IP address, the IP address will have to be reconfigured.

GUI

Once you have successfully accessed the Web GUI and logged in, the management interface may be set by clicking click **System > External Interface** and adjust the IP address settings as required.



CLI

To configure via the CLI, use the following commands and syntax:

```
config system interface
   edit "mgmt1"
      set type physical
      set ip 192.168.0.198 255.255.255.0
      set allowaccess ping https ssh snmp http
      end
```

In 1.0 GA, the configuration of the management interface was achieved via the network settings wizard on the Dashboard.

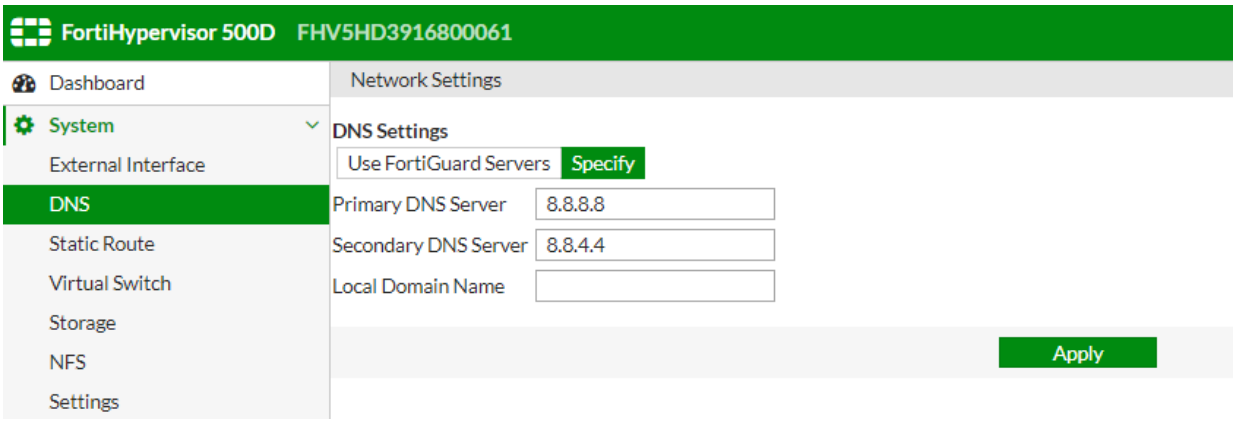
Reconnect the FortiHypervisor device to the network which has just been configured and reconnect to the new GUI IP address.

Configuring DNS

Once complete, configure DNS for the correct settings for your network (not required if DHCP configuration is set).

GUI

In the GUI go to **System > DNS**. You can either **Use FortiGuard Servers** for DNS or you can **Specify** a primary and secondary DNS server or your choice.



CLI

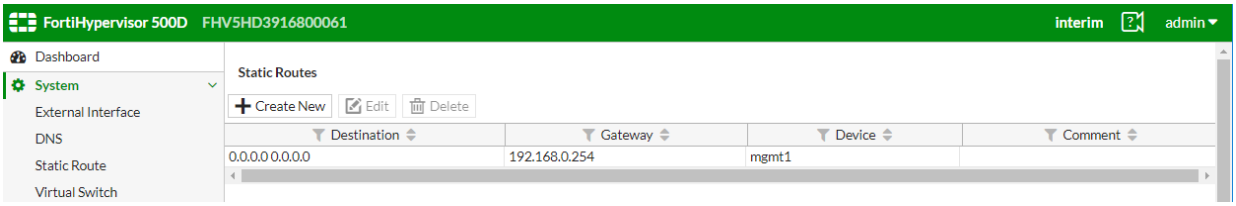
To configure the DNS using the CLI, use your favorite console to connect to the FortiHypervisor through SSH or use the console function and enter the following commands:

```
config system dns
   set primary 8.8.8.8
   set secondary 8.8.4.4
   end
```

Configuring the Default Route

Complete the basic network configuration by setting the correct default route for your network.

GUI



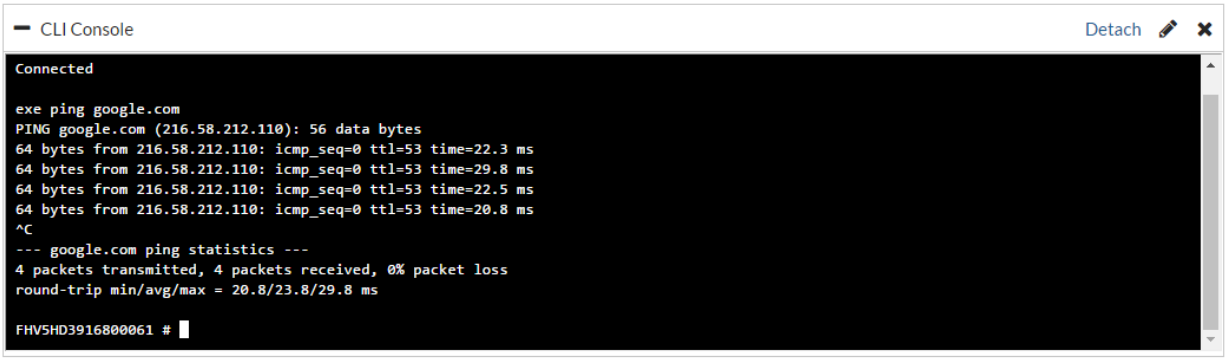
CLI

To configure via the CLI:

```
config router static
   edit 1
      set gateway 192.168.0.254
      set device "mgmt1"
      end
```

Verification of connectivity

Once complete, verify external connectivity, ping an external IP from the Dashboard console.

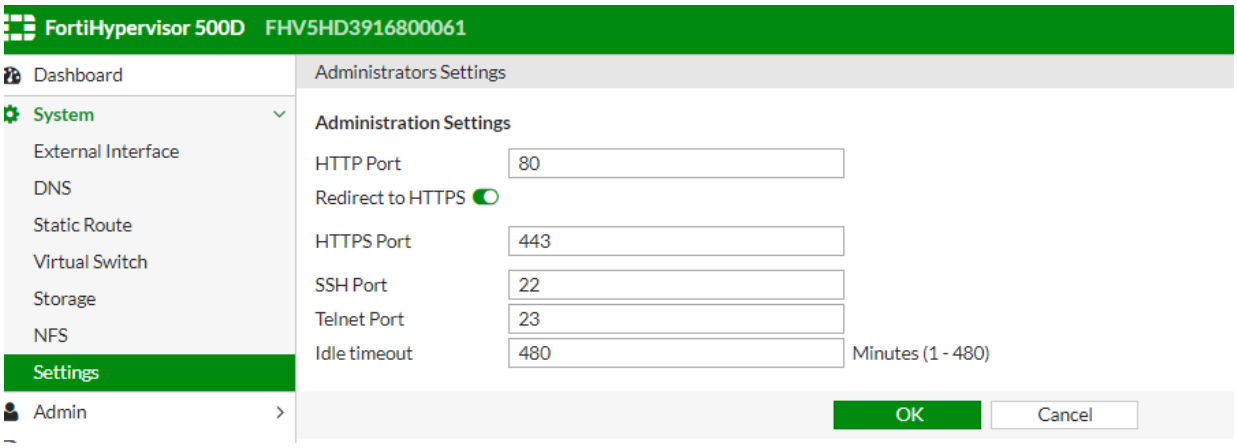


Admin timeout

FortiHypervisor is an appliance designed to host virtual network functions securely. As a result, in line with other Fortinet products and general best practice the default administration timeout is set to 5 minutes. When commissioning FortiHypervisor appliances, in may be necessary to increase the GUI login idle timeout. This is often necessary as the admin session can timeout when uploading large VM images or ISO files. This will cause the upload to fail.

GUI

For version 1.1 and later, the administration time out can be set by going to **System > Settings**, and editing the **Idle timeout** value.



CLI

The administration timeout can be achieved through the CLI, by using your favorite terminal utility. Use the following syntax.

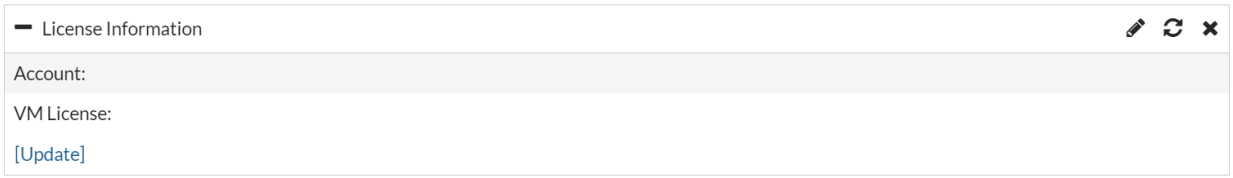
```
config system global
   set admintimeout <number of minutes>
   end
```

The CLI uses the same 1 to 480 minute range of possible values.

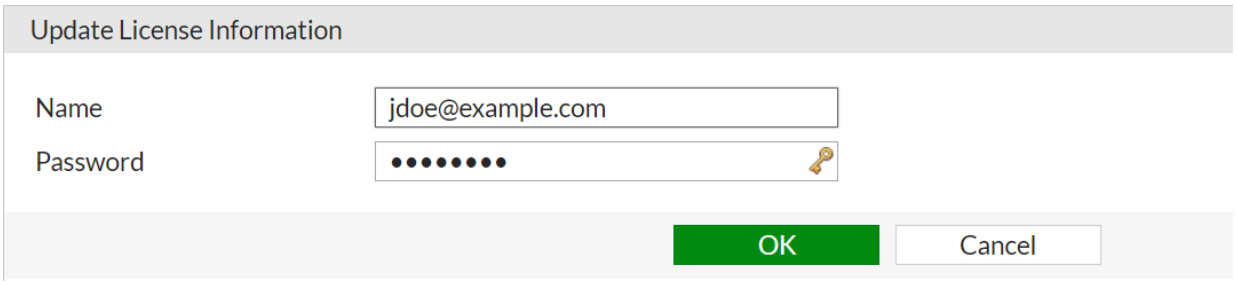
License information

To automatically provision registered licenses into Fortinet VMs from the FortiHypervisor GUI, it is necessary to register the FortiHypervisor in your FortiCare Support account.

On the **Dashboard**, select **[Update]** in the **License Information** widget.



In the **Update License Information** dialogue, enter your FortiCare Support Account details.



Once registered, your VM licenses will be displayed in the **Dashboard** and will be able to be provisioned into Fortinet VMs.

Swap file configuration

The use of a swap file began in version 1.1 to allow the FortiHypervisor to handle high memory load situations. By default, a 4GB swap file is created, this can be modified using the CLI command:

```
config system global
   set swap-size <Memory size 0-64 (GB)>
   end
```

Changes made take effect on reboot.

SNMP Monitoring

SNMP traps and queries may be used to monitor the operational status of the FortiHypervisor platform. SNMP v1, v2, and v3 are supported, along with the following MIBs:

- RFC 1213 MIB-II
- Fortinet Private Enterprises CORE-MIB
- Fortinet Private Enterprises FORTIGATE-MIB

In version 1.1 and higher, the SNMP agent many be enabled on the CLI as shown below.

```
config system snmp sysinfo
   set status enable
   end

config system snmp community
   edit 1
      set name "public"
         config hosts
            edit 1
               set ip 192.168.0.162 255.255.255.255
               end
            end
```

REST API

One of the key advantages of the FortiHypervisor platform is its ability to scale vertically and horizontally. Horizontal scaling can be achieved programmatically by deploying many FortiHypervisor instances and associated virtual network functions in parallel.

FortiHypervisor exposes programmatic feature configuration via a RESTful Web API. The following RESTful APIs are supported by FortiHypervisor:

- **CMDB API**
  - Retrieve object meta data (default, schema)
  - Retrieve object/table (with filter, format, start, count, other flags)
  - Create object
  - Modify object
  - Delete object
  - Clone object
  - Move object
- **Monitor API**
  - Retrieve/Reset endpoint stats (with filter, start, count)
  - Perform endpoint operations
  - Upload/Download files

- Restore/Backup config
- Upgrade/Downgrade firmware
- Restart/Shutdown FHV
- Create/Modify/Delete VMs
- Start/Restart/Shutdown/PowerOff VMs

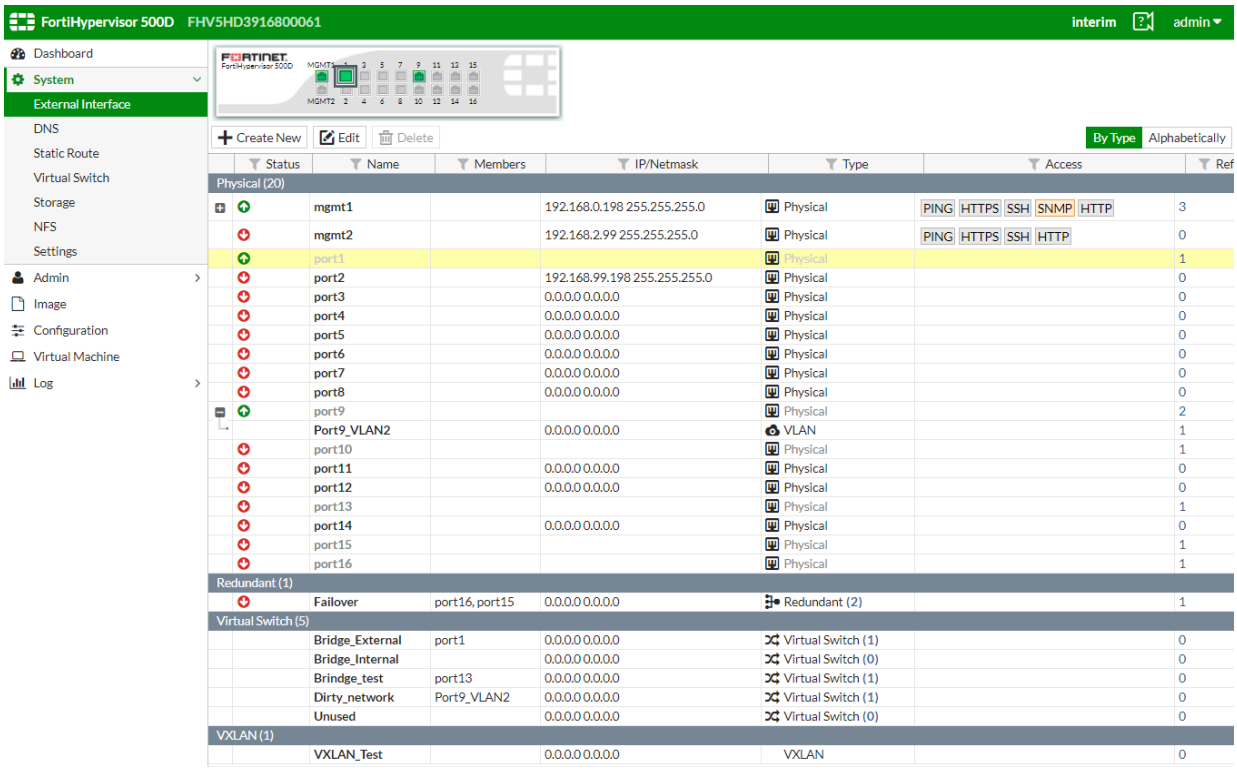
Detailed documentation of the FortiHypervisor REST API is available via the Fortinet Developer Network.

Virtual Networking

External Interfaces

External interfaces refer to the NICs directly attached to the FortiHypervisor platform. External interfaces allow the FortiHypervisor host and associated virtual network functions and VMs to communicate with the outside world, via a connection to an upstream network. Virtual interfaces such as VLAN and VXLAN may be attached to a physical interface.

All physical interfaces on FortiHypervisor can be viewed and configured under **System > External Interfaces**.



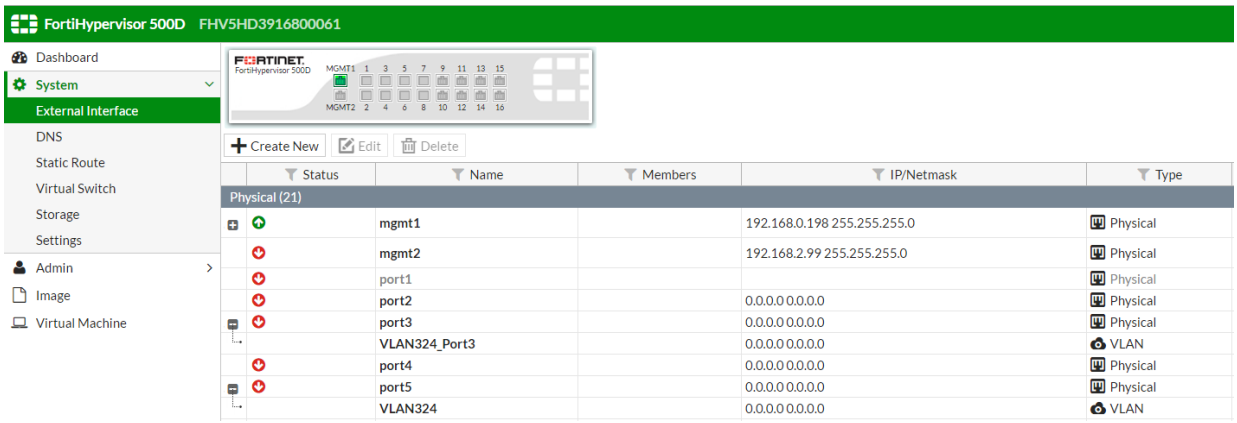
Creating new interfaces

It is possible to create new interface types for which can be connected to configured VMs:

VLAN Interfaces

A virtual LAN (VLAN) allows a subset of network elements to communicate with each other over a shared network. FortiHypervisor supports the attachment of VLAN IDs 0 – 4094 to the physical interfaces.

The same VLAN ID can exist on different interfaces and virtual switches, however, the interface name must be unique.



802.3ad Interfaces

IEEE 802.3ad link aggregation enables ethernet interfaces to be grouped at the physical layer to form a single link layer interface, also known as a link aggregation group (LAG) or bundle. This interface uses Link Aggregation Control Protocol (LACP) to aggregate the interface and control the load distribution or packets across the interface group. Up to 10 interfaces can be configured in LAG.

Packets are load distributed by using a hashing algorithm based on the source/destination IP and ports of the packet.

An 802.3ad interface group provides both resilience and scaling of internet throughput.

Redundant interfaces

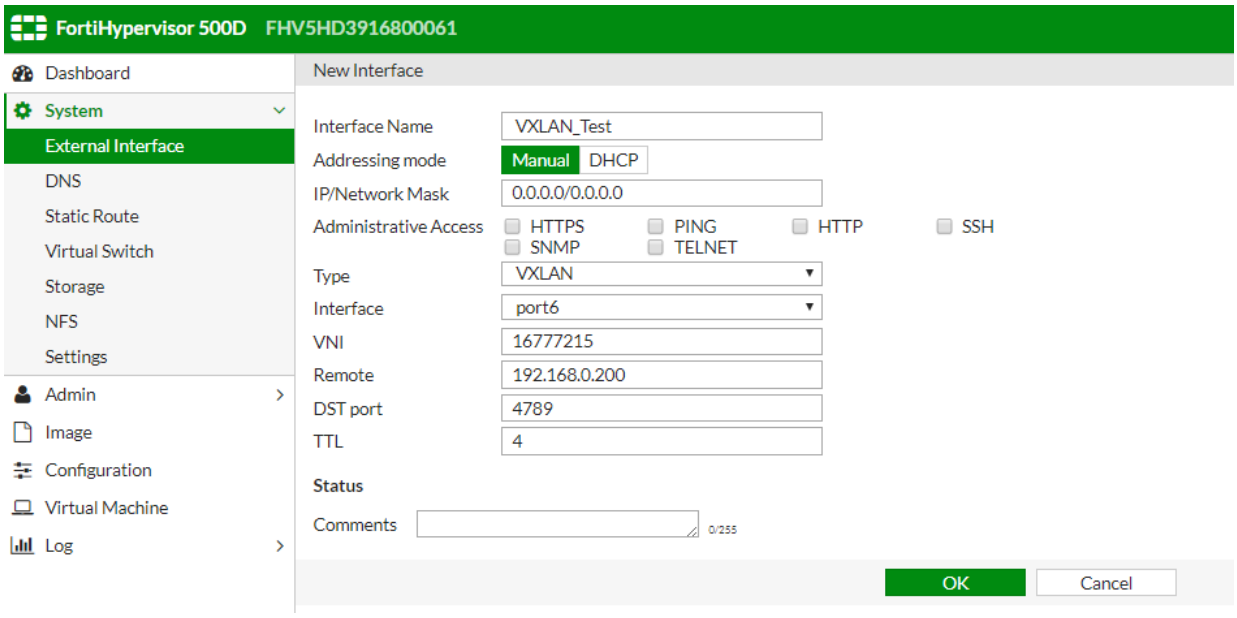
The redundant interface configuration allows multiple interfaces to be grouped together in a similar way to 802.3ad, however they are not all active. Redundant interfaces operate in an Active-Passive configuration only, failing over when the active link fails.

A redundant interface group provides resilience only.

VXLAN Interfaces

VXLAN (Virtual Extensible LAN) is similar to VLANs in that it allows network elements to communicate privately over a shared medium, however it provides much greater capability. VXLAN allows overlaying a Layer 2 (L2) network over a Layer 3 (L3) network using any IP routing protocol. It works by using MAC-in-UDP Encapsulation of traffic enabling the layer 2 data link layer to be extended anywhere in an IP network.

Name:	Name for the VXLAN interface
Interface:	Logical interface where the encapsulation and de-encapsulation occurs.
VNI:	Virtual Network ID 24bit integer: 1-16777215)
Remote DST Port:	IP or address of the remote VTEP (Virtual Tunnel Endpoint) Destination tunnel port (default: 4789)
TTL:	TTL to use in the inner VXLAN network. (outer TTL is unaffected). Default set to 4 to avoid some potential multicast issues.



Virtual Switch

Virtual switches are used to connect Virtual machines to each other and the outside world and may include one or more external (physical) interfaces, although this is not a requirement.

There are two modes that FortiHypervisor virtual switches interface can operate.

Bridge

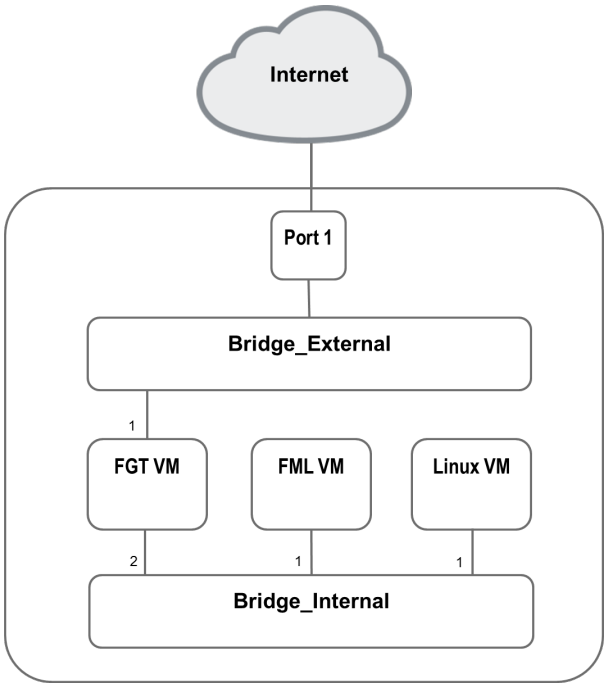
The most common configuration mode is to associate an interface as part of a bridge where all interfaces configured in that bridge are part of a shared Layer2 broadcast domain.

External Interfaces (Physical, VLAN, 802.3ad and Redundant) can all be part of a bridge virtual switch. A virtual machine interface can be connected to a bridge with or without an External Interface

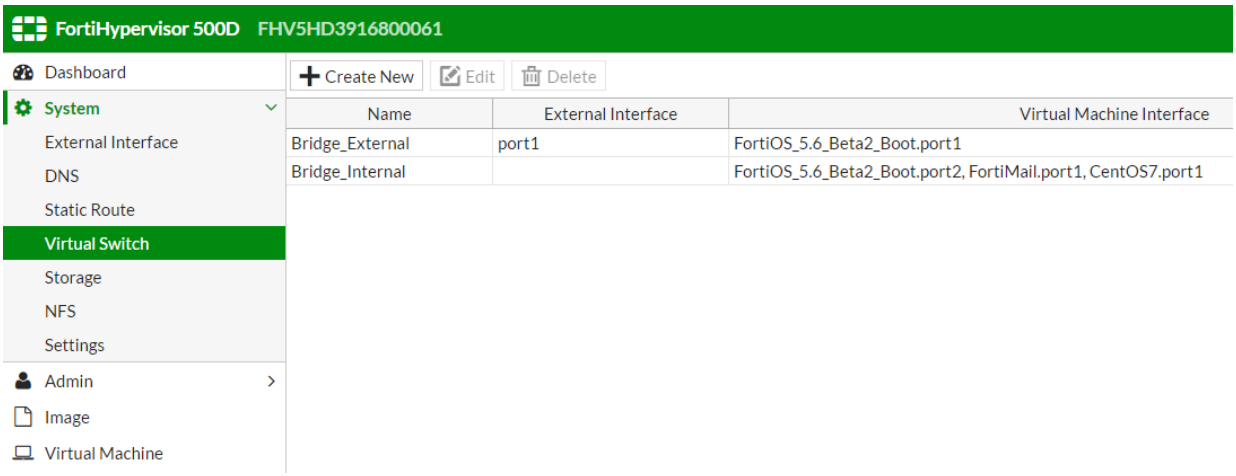
In the following example, the FortiGate VM Port1 interface is connected to the Virtual Switch “Bridge_External” which is also connected to the External Interface Port 1 which is a physical interface connected to the internet.

There is a second Virtual Switch “Bridge_Internal” which is only used to internally connect VM interfaces

For the FortiMail and Linux VM to communicate with the Internet, the FortiGate would need to be configured to route and allow this traffic.

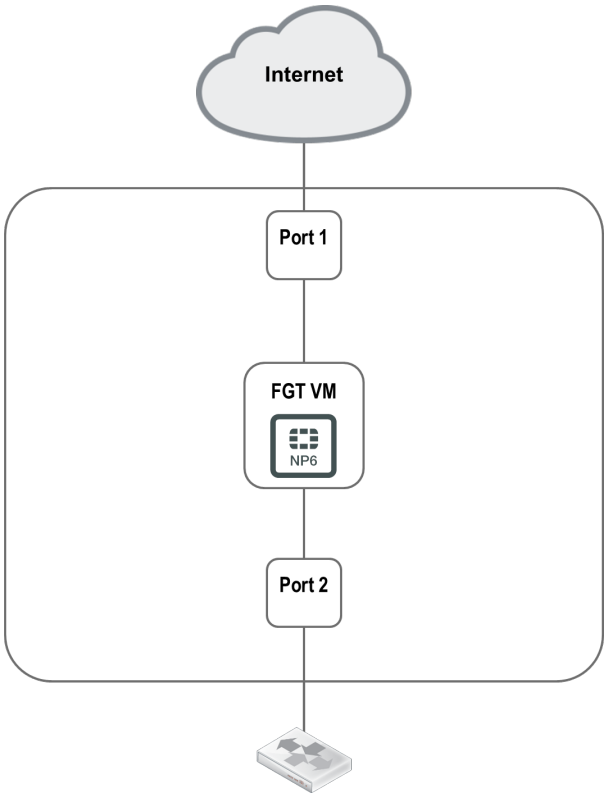


The configuration described would appear as shown below in the FortiHypervisor GUI. Note that only Bridge_External has an External Interface connected as Bridge_Internal is purely a virtual switch used to interconnect the VMs.



Passthrough

Passthrough mode directly connects a VM interface to an External Interface without the need for an intermediary Virtual Switch. Passthrough mode is a pre-requisite for FortiOS to offload network performance to the NP6 FortiASIC.


Internet
Port 1
FGT VM
NP6
Port 2

Virtual Machines

Provisioning Virtual Machines

This section will detail the methods for installing FortiGate/FortiOS and other Fortinet VNFs and thirty party VMs into FortiHypervisor.

There are 2 areas in which VMs are configured in FortiHypervisor.

Image

The Image menu, is where Fortinet and third party VM disks are uploaded [Upload] and empty disks created [Create New]. This is also where ISO files can be uploaded for use in installing an OS into a virtual machine.

VM disks should be uploaded in uncompressed KVM QCOW2 format and CD/DVDs in ISO9660 format.

Virtual Machines

The Virtual Machines menu is where VM are configured. A VM configuration includes definition of the number of CPUs and RAM provisioned, disks to be used, any CDROMs mounted and which network interfaces configured.

For systems with an active fortiCare support account attached, It is possible to provision a new Fortinet VM directly from FortiGuard using the Virtual Machines menu, bypassing the need to manually upload the disk images.

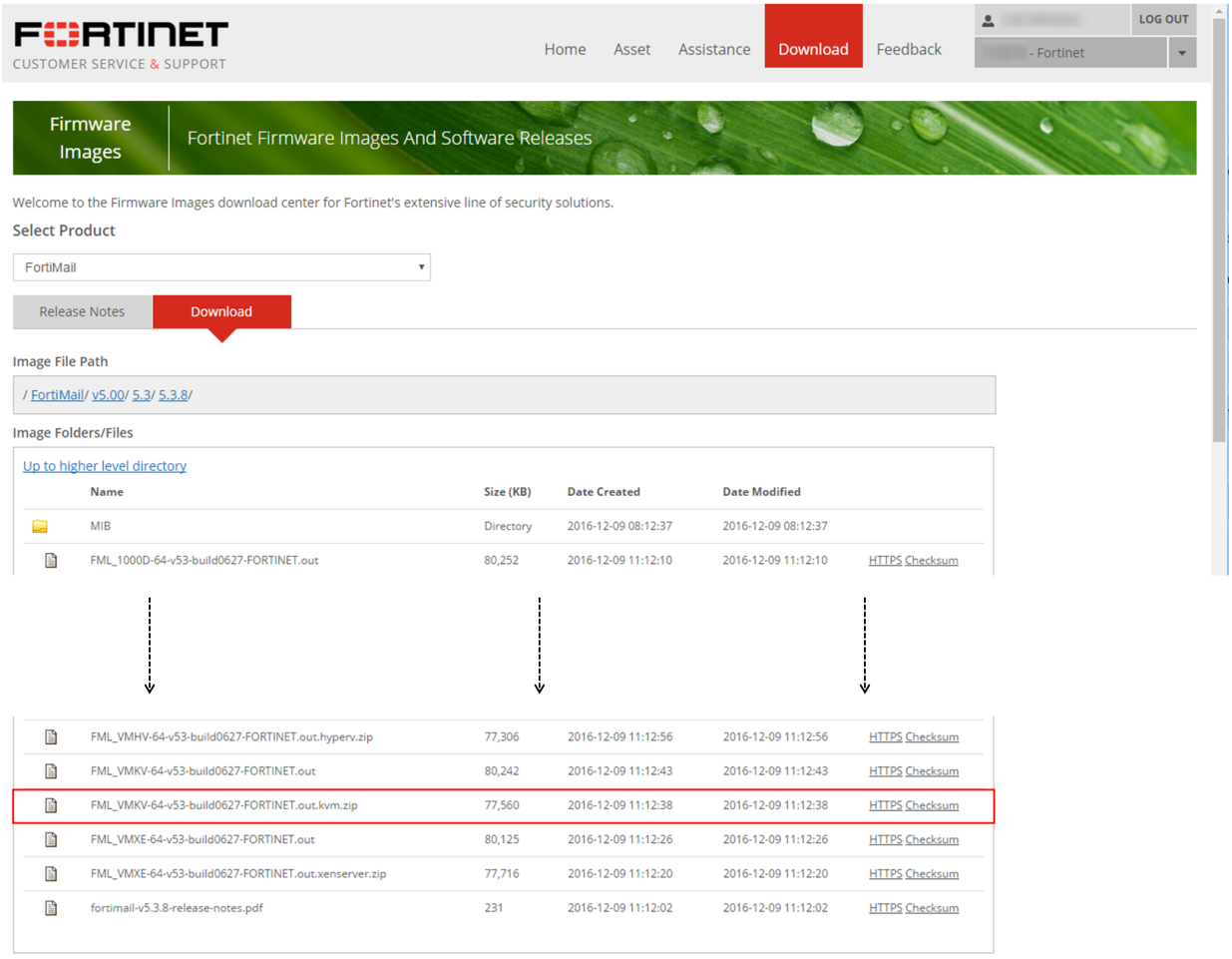
Note that when provisioning CPU resource, it is possible to overcommit resource i.e. so more CPUs are specified that are physically available. Please be aware of the consequence of such configuration. Memory cannot be overcommitted at this time and is limited to being configured to 100% of the available resource minus 2GB which is reserved for system use.

Installing Fortinet VMs

Manual Upload

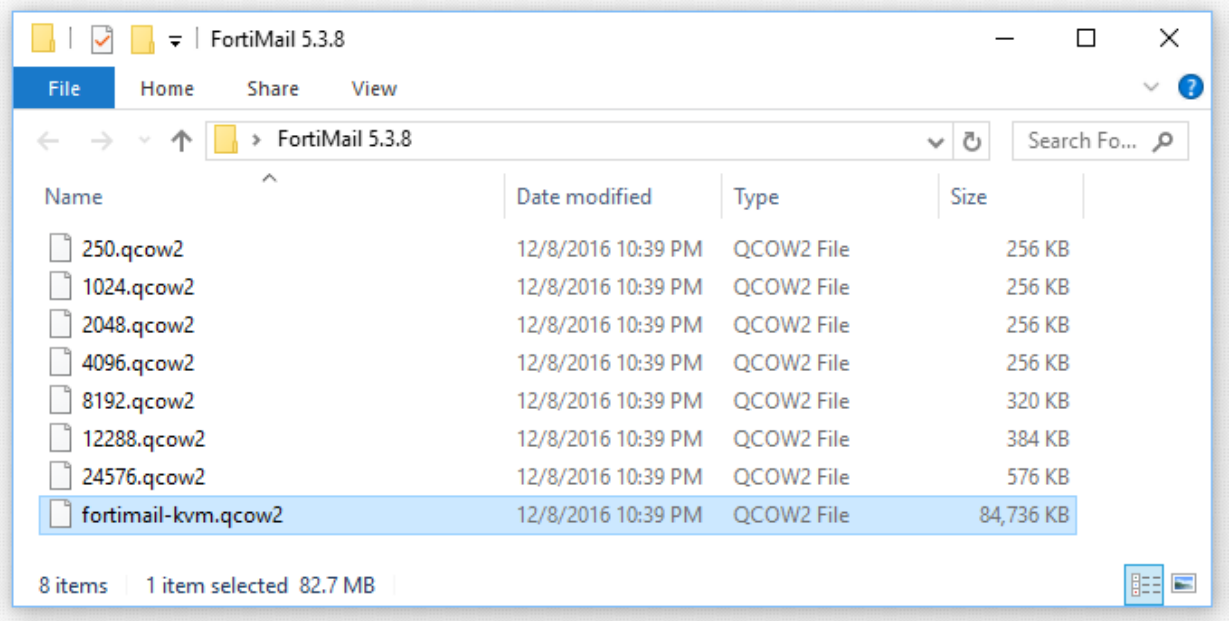
If a Fortinet VM is not available to be imported automatically, use this method to manually import the Fortinet VM.

1. Locate and download the KVM version of the required VM from the **Download > Firmware Images** section of the Fortinet Support site e.g. for FortiMail 5.3.8:



2. Once downloaded, extract the zip file to a folder on your management computer.

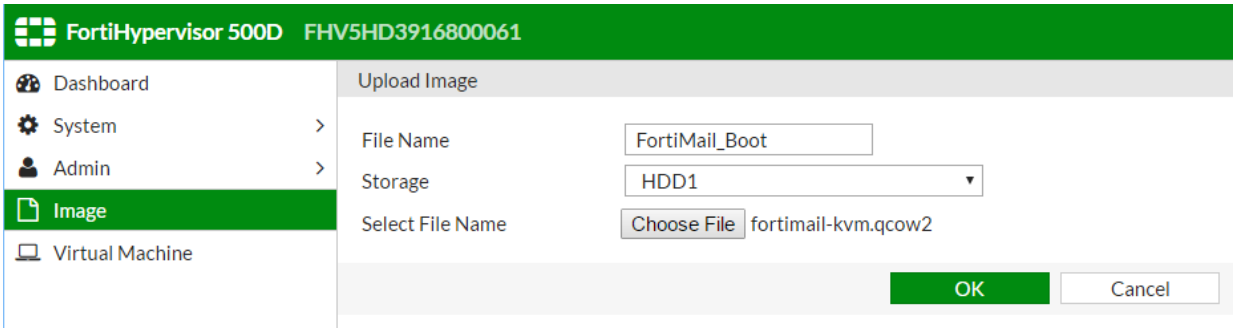
It is worth drawing attention to the step about the extraction of the zip file. The process only works if the file(s) contained in the zip file are used for the installation, not the zip file itself.



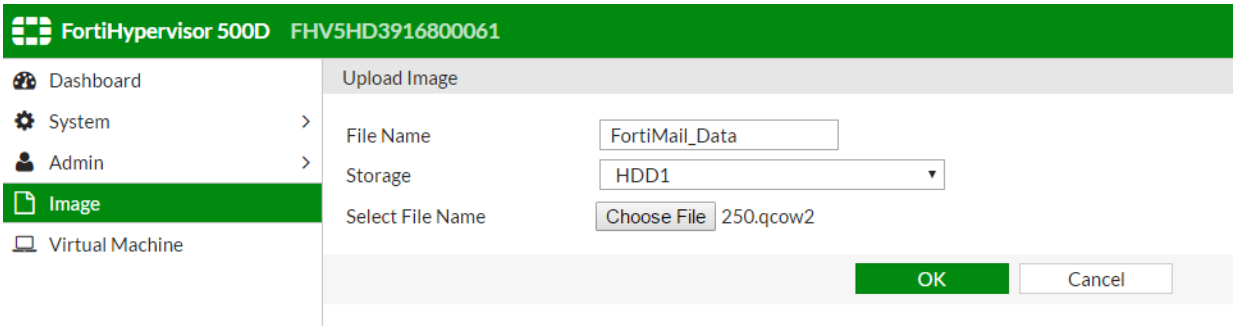
VMs such as FortiOS, FortiManager and FortiCache only have a single boot disk and data disks need to be created manually to the required size. Some VMs such as FortiMail have pre-defined disk templates of varying sizes which can optionally be used to provision the data disks for a VM install.

`fortimail-kvm.qcow2`	FortiMail boot disk
`250 - 24576.qcow2`	FortiMail data disk template in sizes from 250GB to 24TB

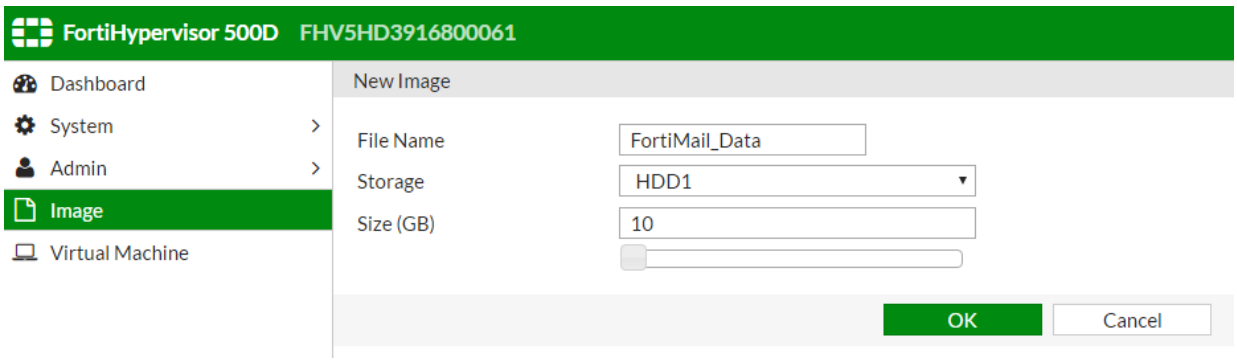
3. Upload the boot disk to the FortiHypervisor by selecting **Image > [Upload]**.



4. Repeat the process for the data disk using one of the provided templates as shown:

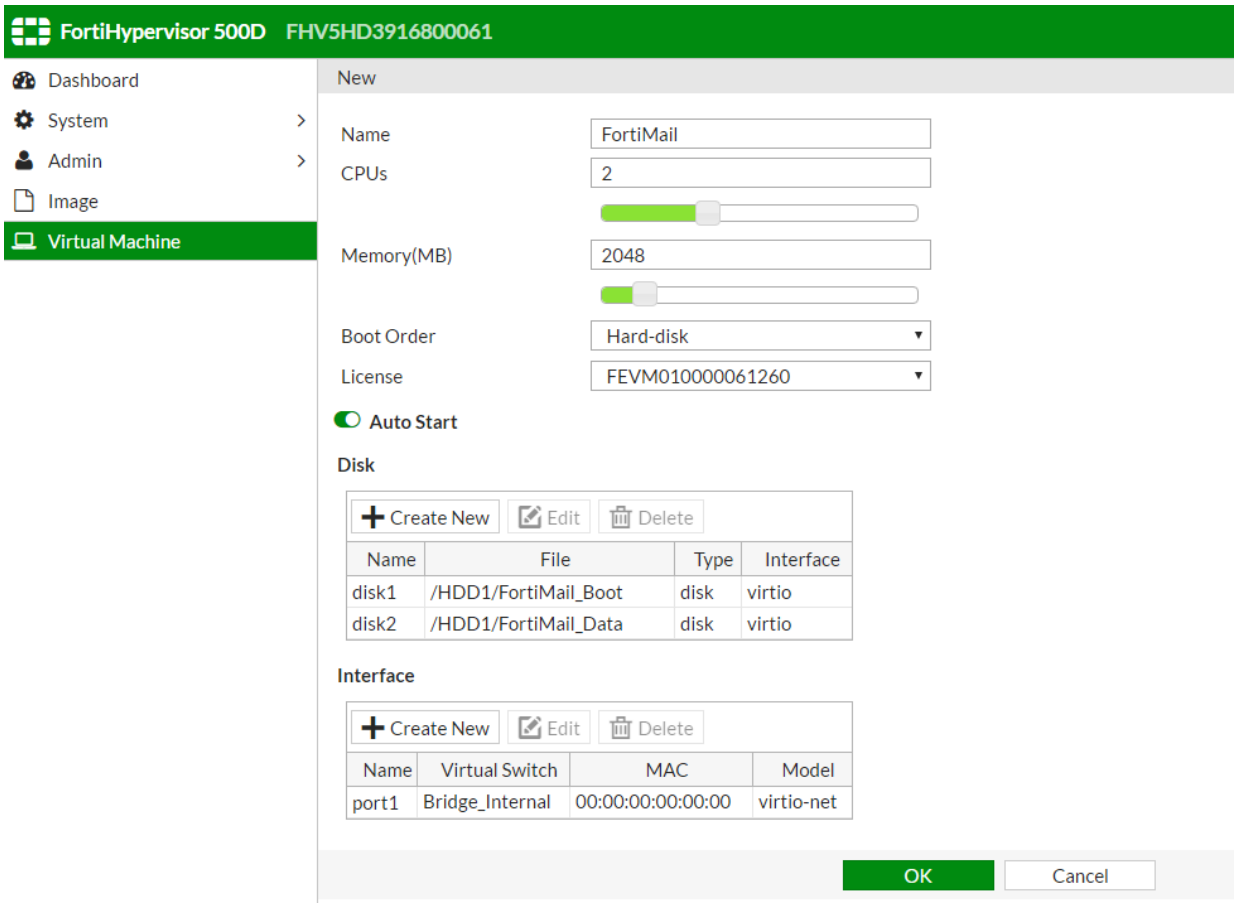


Alternatively, manually create a disk with whatever disk size is required by selecting Image > [Create New].



5. Once the disks have been configured, proceed to the **Virtual Machine > [Create New]** to provision the VM.

CPU:	Select the number of CPUs to suit your environment and VM license
Memory:	Select the amount of memory to suit your environment and VM license
Boot Order	Select the boot order of Hard-Disk or CDROM. In the Fortinet VM case this is always Hard-Disk.
License:	If the FortiHypervisor is correctly associated with a FortiCare account, any supported VM licenses should appear here. These licenses can be selected and automatically configured into the VM using cloud-init for supported Fortinet VMs.
AutoStart:	Start the VM once configuration has been completed?
Disk:	Select Create New and bind the previously uploaded Boot disk and data disk(s) (VM dependent) • Select the disk type according to the VM being configured. • For Fortinet VMs this is normally Virtio however see Appendix X for exceptions.
Interface:	Select Create New and bind the appropriate Virtual Switch interfaces to the VM • Select the interface type according to the VM being configured. • For Fortinet VMs this is normally Virtio-net howver, refer to **Appendix A** for exceptions.



Installing Third Party VMs

Installing via ISO

This example uses the CentOS7 ISO image as an example, however this method is transferrable to other x86 based ISO installs.

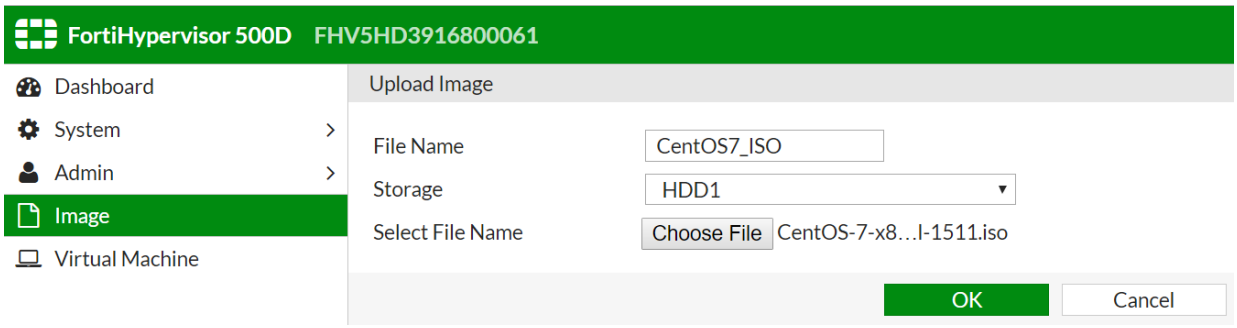
A minimum of two disks are required for an ISO based install:

• The ISO image to perform the initial install boot from

• The disk to which the VM will be installed

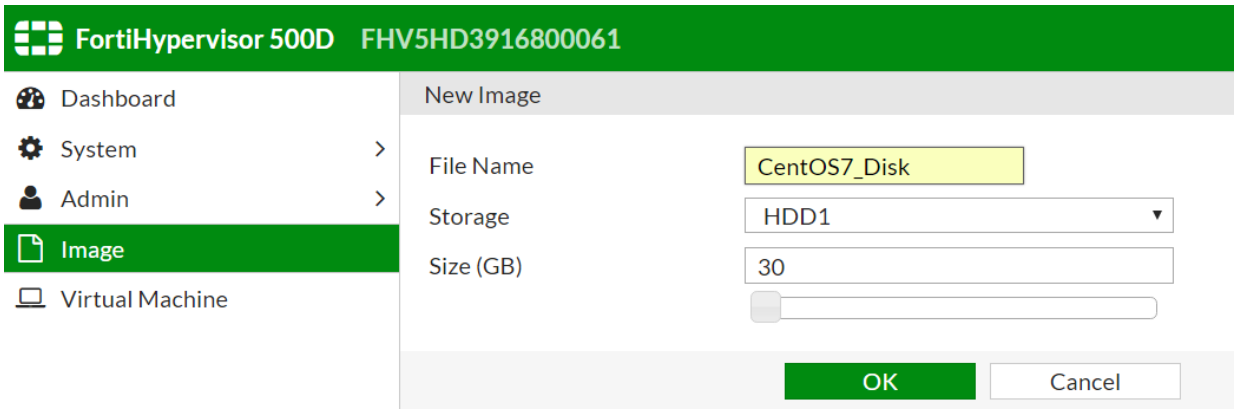
1. **Upload ISO Image**

Select **Virtual Machine > [Upload]** and upload the chose ISO Image, in this example `CentOS-7-x86_64-NetInstall-1511.iso`.



2. Create Installation disk

Create a disk to which the ISO image will be installed. Select the appropriate disk size according to the requirements of the Guest VM being installed.



3. Configure VM

Once the disks have been configured, proceed to the **Virtual Machine > [Create New]** to provision the VM.

CPU: Select the number of CPUs to suit your environment and VM license

Memory: Select the amount of memory to suit your environment and VM license

Boot Order Select the boot order of Hard-Disk or CDROM. In the ISO case, set this to CDROM

License: This is not relevant for an ISO install, leave empty.

AutoStart: Set start the VM once configuration has been completed.

Select Create New and bind the previously uploaded Boot disk and data disk(s) (VM dependent)

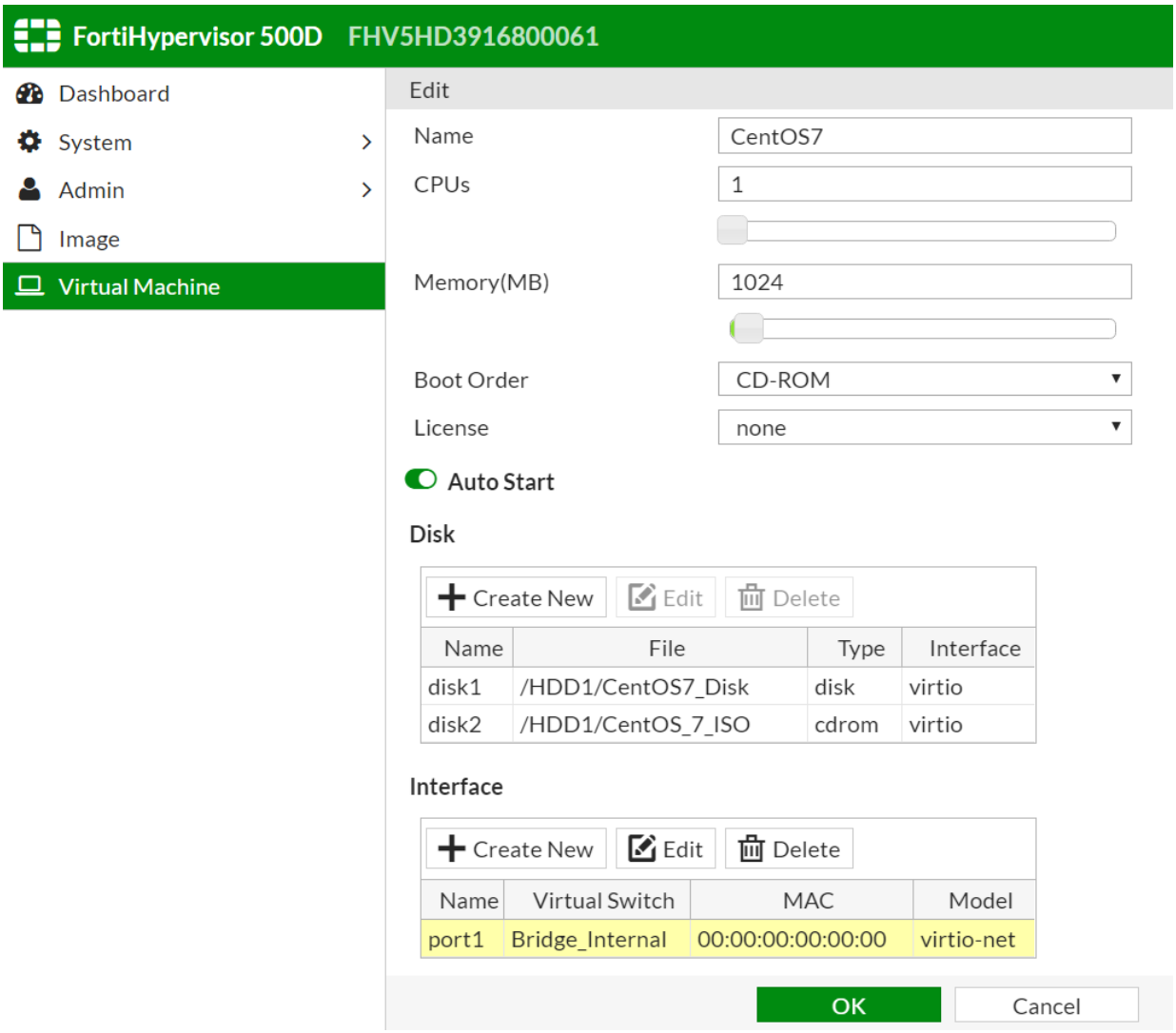
Disk:

- Select the disk type according to the VM being configured.
  - For compatibility, set this to IDE.
  - For performance, set this to Virtio (if your VM supports this hardware type).

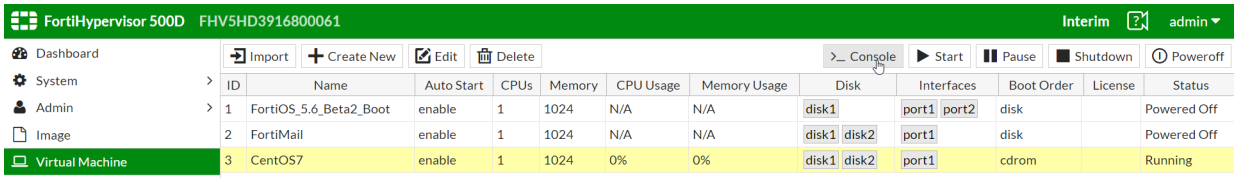
Select Create New and bind the appropriate Virtual Switch interfaces to the VM

Interface:

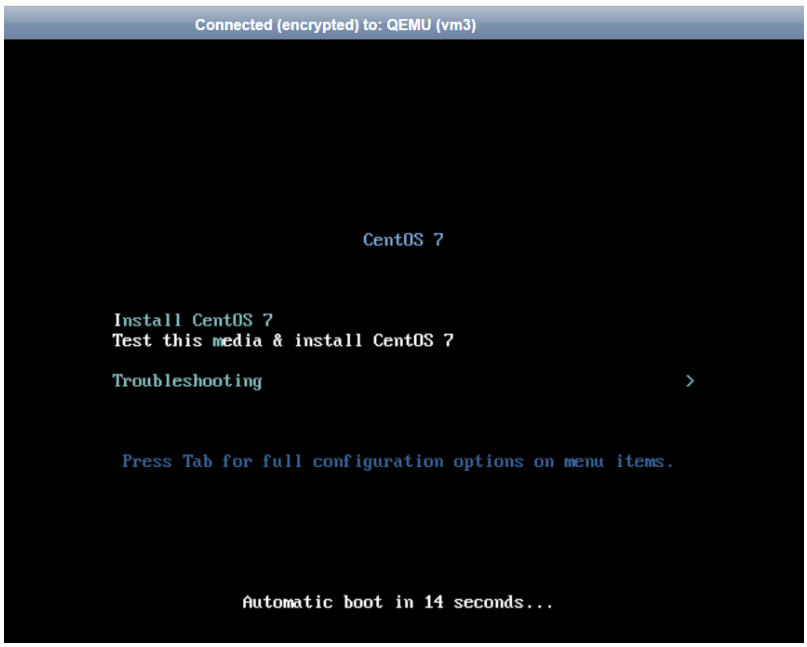
- Select the interface type according to the VM being configured.
  - For compatibility, set this to E1000 (or RT8139).
  - For performance, set this to Virtio-net (if your VM supports this hardware type).



4. On completion the ISO will begin to boot. Select the VM and click **[>_Console]** .



5. Follow the ISO install instructions or on-screen commands to complete the VM install process.



6. Once the installation is complete, power off the VM and change the boot order to prioritize boot from Hard Disk instead of CDROM. The CDROM drive can be removed if no longer required.

Appendix A

Tested Fortinet VM Configurations

VM	Disk	Network	Notes
FortiManager KVM 5.4.1	Virtio	Virtio-net	
FortiAnalyzer KVM 5.4.1	Virtio	Virtio-net	
FortiGate KVM 5.4.1	Virtio	Virtio-net	
FortiWeb KVM 5.6.0	Virtio	Virtio-net	
FortiADC KVM 4.6.0	Virtio	Virtio-net	
FortiRecorder KVM 2.4.1	Virtio	Virtio-net	
FortiVoice KVM 5.2.2	Virtio	Virtio-net	
FortiVoice Enterprise KVM 5.0.5	Virtio	Virtio-net	
FortiMail KVM 5.3.6	Virtio	Virtio-net	
FortiAuthenticator 4.3.0	Virtio	Virtio-net	
FortiCache KVM 4.2.2	Virtio	Virtio-net	
FortiWLM KVM 8.3	Virtio	Virtio-net	

Tested Third Party VM Configurations

Operating Systems

VM	Disk	Network	Notes
Windows Server 2012 R2	IDE	E1000	ISO Install
Windows 10 Pro	IDE	E1000	ISO Install
Windows 7 Pro	IDE	E1000	ISO Install

VM	Disk	Network	Notes
CentOS 7	Virtio	Virtio-net	ISO Install from Netinstall image (Install Type Network Server with GUI
Ubuntu 16.04	Virtio	Virtio-net	ISO Install from Netinstall image (Install Type Network Server with GUI)
Tiny Core Linux 6.4	Virtio	Virtio-net	Prebuilt KVM
Alpine Linux 3.2.3	IDE	Virtio-net	Prebuilt KVM
OpenBSD 6.0	IDE	E1000	ISO Install
VMWare ESXi 6.5	IDE	E1000	ISO Install

Application VMs and VNFs

VM	Disk	Network	Notes
VeloCloud Edge 2.2.1 SD-WAN	Vertio	Vertio-net	Tested successfully
SilverPeak SD-WAN	Vertio	Vertio-net	Tested successfully
Nozomi SCADAguardian	Vertio	Vertio-net	Tested successfully

Is there is a third party VM not covered here which you would like to see officially validated, please feedback via your Fortinet Account Team.

Unsupported VMs

VM	Disk	Network	Notes
Windows 8 Pro	IDE	E1000	Install hangs at Configuring Devices. Investigating

Appendix B

FHV-500D

The command `diagnose npu np6 port-list` produces a table with the following information.

Chip	XAUI	Ports	Max Speed	Cross-chip offloading
np6 0	0			
np6 0	1	port1	1 G	Yes
np6 0	1	port2	1 G	Yes
np6 0	1	port3	1 G	Yes
np6 0	1	port4	1 G	Yes
np6 0	1	port5	1 G	Yes
np6 0	1	port6	1 G	Yes
np6 0	1	port7	1 G	Yes
np6 0	1	port8	1 G	Yes
np6 0	1	port9	1 G	Yes
np6 0	1	port10	1 G	Yes
np6 0	1	port11	1 G	Yes
np6 0	1	port12	1 G	Yes
np6 0	1	port13	1 G	Yes
np6 0	1	port14	1 G	Yes
np6 0	1	port15	1 G	Yes
np6 0	2			
np6 0	3			

FHV-2500E

The command `diagnose npu np6 port-list` produces a table with the following information.

Chip	XAUI	Ports	Max Speed	Cross-chip offloading
np6 0	0	port37	10 G	No
np6 0	1	port38	10 G	No
np6 0	2	port39	10 G	No
np6 0	3	port40	10 G	No
-	-	-	-	-
np6 1	0	port1	1 G	Yes
np6 1	0	port5	1 G	Yes
np6 1	0	port9	1 G	Yes
np6 1	0	port13	1 G	Yes
np6 1	0	port17	1 G	Yes
np6 1	0	port21	1 G	Yes
np6 1	0	port25	1 G	Yes
np6 1	0	port29	1 G	Yes
-	-	-	-	-
np6 1	1	port2	1 G	Yes
np6 1	1	port6	1 G	Yes
np6 1	1	port10	1 G	Yes
np6 1	1	port14	1 G	Yes
np6 1	1	port18	1 G	Yes
np6 1	1	port22	1 G	Yes
np6 1	1	port26	1 G	Yes
np6 1	1	port30	1 G	Yes

Chip	XAUI	Ports	Max Speed	Cross-chip offloading
-	-	-	-	-
np6 1	2	port3	1G	Yes
np6 1	2	port7	1G	Yes
np6 1	2	port11	1G	Yes
np6 1	2	port15	1G	Yes
np6 1	2	port19	1G	Yes
np6 1	2	port23	1G	Yes
np6 1	2	port27	1G	Yes
np6 1	2	port31	1G	Yes
-	-	-	-	-
np6 1	3	port4	1G	Yes
np6 1	3	port8	1G	Yes
np6 1	3	port12	1G	Yes
np6 1	3	port16	1G	Yes
np6 1	3	port20	1G	Yes
np6 1	3	port24	1G	Yes
np6 1	3	port28	1G	Yes
np6 1	3	port32	1G	Yes
-	-	-	-	-
np6 2	0			
np6 2	1			
np6 2	2	port41	10 G	No
np6 2	3	port42	10 G	No
-	-	-	-	-
np6 3	0	port33	10 G	No

FORTINET

High Performance Network Security